IN THE CLAIMS:

This listing of claims will replace all prior versions, and listings, of claims in the application:

1. - 24. (Cancelled).

25. (Currently Amended) An enciphering method ~~according to claim 23, further~~ comprising:

keeping a plurality of second keys;

enciphering data with a first key;

enciphering said first key with a p number of second keys, where p is an integer greater than or equal to two, of the kept plurality of second keys to obtain a p number of enciphered first keys, respectively; and

selecting part of said plurality of second keys as said p number of second keys for use in enciphering said first key in a case where part of said plurality of second keys has been broken.

26. – 28. (Cancelled).

29. (Currently Amended) A recording medium manufacturing method ~~according to claim 28, further~~ comprising:

keeping a plurality of second keys;

obtaining first information composed of enciphered data by enciphering data with a first key;

obtaining second information composed of a p number of enciphered first keys, where p is an integer greater than or equal to two, obtained by enciphering said first key with a p number of second keys of the kept plurality of second keys, respectively;

recording said first and second information on the same recording medium; and

selecting part of said plurality of second keys as said p number of second keys for use in enciphering said first key in a case where part of said plurality of second keys has been broken.

30. – 31. (Cancelled).

32. (Currently Amended) A deciphering method comprising:

recording at least part of a p number of second keys, where p is an integer geater than or equal to two, in a secret area in a deciphering device;

inputting first information composed of enciphered data obtained by enciphering data with a first key and second information composed of a p number of enciphered first keys obtained by enciphering said first key with said p number of second keys, respectively;

deciphering at least one said p number of enciphered first keys using the recorded at least part of the p number of second keys to obtain said first key;

confirming by a specific method that the obtained first key is correct; and

deciphering said enciphered data using said obtained first key after the confirmation to obtain said data.

33. (Previously Presented) A deciphering method according to claim 32, wherein said data includes at least one of key information, documents, sound, images, and programs.

34. (Currently Amended) A deciphering device comprising:

a recording unit configured to record at least part of a p number of second keys, where p is an integer greater than or equal to two, in a secret area in the deciphering device;

an input unit configured to input first information composed of enciphered data obtained by enciphering data with a first key and second information composed of a p number of enciphered first keys obtained by enciphering said first key with said p number of second keys, respectively; and

a deciphering unit configured to decipher at least one of said p number of enciphered first keys of said second information inputted from said input unit using the recorded at least part of the p number of second keys in said recording unit, confirm by a specific method that the obtained first key is correct, and decipher said enciphered data of said first information using said first key after the confirmation to obtain said data.

35. (Currently Amended) A recording and reproducing device comprising:

a recording unit configured to record at least part of a p number of second keys, where p is an integer greater than or equal to two, in a secret area in the recording and reproducing device;

a reading unit configured to read first information composed of enciphered data obtained by enciphering data with a first key and second information composed of a p number of enciphered first keys obtained by enciphering said first key with a p number of second keys from a recording medium on which said first information and said second information have been stored, respectively, and

a deciphering unit configured to decipher at least one of said p number of enciphered first keys of said second information read by said reading unit using the recorded at least part of the p number of second keys in said storage unit, confirm by a specific method that the obtained first key is correct, and decipher said enciphered data of said first information using said first key after the confirmation to obtain said data.

36. (Previously Presented) A key control method comprising:

causing a first caretaker to take custody of a plurality of second keys;

causing a second caretaker to take custody of first information composed of enciphered data obtained by enciphering data with a first key and second information composed of a p number of enciphered first keys, where p is an integer greater than or equal to two, obtained by enciphering said first key with a p number of second keys of said plurality of second keys, respectively, and

causing a third caretaker to take custody of at least part of said plurality of second keys, said at least part of said plurality of second keys being recorded in a secret area of a device provided by said third caretaker.

37. (Cancelled).

38. (Currently Amended) An enciphering method ~~according to claim 37, further~~ comprising:

keeping a plurality of second keys;

enciphering data with a first key;

enciphering said first key with a p number of second keys, where p is an integer greater than or equal to two, of the kept plurality of second keys to obtain a p number of enciphered first keys, respectively;

recording the enciphered data and the p number of enciphered first keys on a recording medium to be distributed to a user; and

selecting part of said plurality of second keys as said p number of second keys for use in enciphering said first key in a case where part of said plurality of second keys has been broken.

39. – 40. (Cancelled).

41. (Previously Presented) A master key control method comprising:

keeping a plurality of master keys;

allocating at least part of the plurality of master keys to said player maker;

receiving a session key supplied from a disk maker;

selecting part of the plurality of master keys for use in enciphering said session key in a case where part of the plurality of master keys has been broken;

enciphering the received session key with the selected part of the plurality of master keys to produce a plurality of enciphered session keys, respectively; and

supplying the produced plurality of enciphered session keys to said disk maker.

42. (Previously Presented) An enciphering method comprising:

keeping a plurality of second keys;

enciphering data with a first key;

enciphering said first key with a p number of second keys, where p is an integer greater than or equal to two, of the kept plurality of second keys to obtain a p number of enciphered first keys, respectively; and

enciphering said first key with said first key itself.

43. (Previously Presented) A key control method applied to a key control organization, a disk maker, and a player maker, said method comprising:

taking custody of a plurality of master keys by said key control organization, wherein said key control organization allocates part of the plurality of master keys to said player maker, receives a session key supplied from said disk maker, enciphers the received session key with said plurality of master keys to produce first information composed of a plurality of enciphered session keys, respectively, and supplies the produced first information to said disk maker;

providing a player device by said player maker, said player device having one or more master keys that are allocated by said key control organization; and

providing a disk by said disk maker, wherein said disk maker produces the session key and supplies the produced session key to said key control organization, receiving the first information supplied from said key control organization, acquiring second information obtained by enciphering the session key with itself and third information obtained by enciphering data with the session key, and recording the first information, the second information, and the third information onto said disk.

44. (Previously Presented) A key control method according to claim 43, wherein said key control organization allocates a different part of the plurality of master keys exclusively to a plurality of player makers.

45. (Previously Presented) A key control method according to claim 43, wherein in a case where a master key has been broken, said disk maker manufactures a disk without using the broken master key.

46. (Previously Presented) A disk manufacturing method comprising:

producing a session key;

enciphering data with the session key to obtain first information;

supplying the session key to a key control organization;

producing second information by enciphering the produced session key with itself;

receiving from said key control organization, third information composed of a plurality of enciphered session keys obtained by enciphering the supplied session key with a plurality of master keys, respectively; and

recording the first information, the second information, and the third information onto a recording mechanism.

47. (Previously Presented) A disk manufacturing method comprising:

producing a session key;

enciphering data with the session key to obtain first information;

supplying the session key to a key control organization;

received from said key control organization, second information obtained by enciphering the supplied session key with itself;

receiving from said key control organization, third information composed of a plurality of enciphered session keys obtained by enciphering the supplied session key with a plurality of master keys, respectively, and

recording the first information, the second information, and the third information onto a recording medium.